

1/5/1 (Item 1 from file: 351)  
 DIALOG(R) File 351:Derwent  
 (c) 2000 Derwent Info Ltd. All rts. reserv.

010093179 \*\*Image available\*\*  
 WPI Acc No: 1994-360892/199445  
 XRPX Acc No: N94-282782

**Key opening code system - calculates ellipse curve parameter from code sentence and common sentence obtained using calculation theorem**

Patent Assignee: NIPPON TELEGRAPH & TELEPHONE CORP (NITE )

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
JP 6282226	A	19941007	JP 9370436	A	19930329	199445 B

Priority Applications (No Type Date): JP 9370436 A 19930329

Patent Details:

Patent No	Kind	Lan Pg	Main IPC	Filing Notes
JP 6282226	A	12	G09C-001/00	

Abstract (Basic): JP 6282226 A

The open key code system consists of an open file appts. (10) which chooses arbitrary prime numbers. The encryption keys corresp. to arbitrary prime numbers are formed by a key coding appts. (20). The decoding keys corresp. to the prime numbers are stored in a decoding key table of a decoder (40).

The open key of common sentence from the open file appts. is received and multiplied on an ellipse curve by an encryption appts. (30). The output of the encryption appts. is transmitted to the decoder as a code sentence. The ellipse curve parameter from the code sentence is calculated and the decoding key, corresponding to the parameter is selected from the decoding key table. Using a calculation theorem, the common sentence is obtained from the decoder.

ADVANTAGE - Prevents constraint of prime numbers of parameters. Provides safety.

Dwg.1/6

Title Terms: KEY; OPEN; CODE; SYSTEM; CALCULATE; ELLIPSE; CURVE; PARAMETER; CODE; SENTENCE; COMMON; SENTENCE; OBTAIN; CALCULATE; THEOREM

Derwent Class: P85; W01

International Patent Class (Main): G09C-001/00

International Patent Class (Additional): H04L-009/06; H04L-009/14

File Segment: EPI; EngPI

1/5/2 (Item 1 from file: 347)  
 DIALOG(R) File 347:JAPIO  
 (c) 2000 JPO & JAPIO. All rts. reserv.

04610326 \*\*Image available\*\*  
 ELLIPTIC CURVE-BASED PUBLIC-KEY CIPHER SYSTEM

PUB. NO.: 06-282226 JP 6282226 A]

PUBLISHED: October 07, 1994 (19941007)

INVENTOR(s): KUWAKADO SHUSUKE  
 KOYAMA KENJI

APPLICANT(s): NIPPON TELEGR & TELEPH CORP <NTT> [000422] (A Japanese Company or Corporation), JP (Japan)

APPL. NO.: 05-070436 [JP 9370436]

FILED: March 29, 1993 (19930329)

INTL CLASS: [5] G09C-001/00; H04L-009/06; H04L-009/14

JAPIO CLASS: 44.9 (COMMUNICATION -- Other); 44.3 (COMMUNICATION -- Telegraphy)

JOURNAL: Section: , Section No. FFFFFFFF, Vol. 94, No. 10, Pg. FFFFFFFF, FF, FFFF (FFFFFFFFF)

## ABSTRACT

PURPOSE: To provide an elliptic curve-based public-key enciphering system having much enhanced safety by eliminating a limit to the prime factor of a parameter.

CONSTITUTION: An arbitrary prime factor is first selected and an enciphering key corresponding to the factor is registered with a public file device 10. Then, a decoding key list corresponding to the factor and the enciphering key is generated and saved in a decoding device 40, together with the factor. Thereafter, an enciphering device 30 receives the public-key of a receiver (decoding device) from the public file device 10, and performs the multiplication of a plain text on an elliptic curve. Then, the device 30 sends the multiplied value as a cryptotext to the decoding device 40. This device 40 calculates an elliptic curve parameter from the cryptotext and selects such a decoding key as corresponding to the parameter, using the decoding key list. Then, the plain text is obtained from the multiplied value of the cryptotext on the elliptical curve, using a remainder theorem.

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平6-282226

(43)公開日 平成 6 年(1994)10月 7 日

(51)Int.Cl.<sup>5</sup>

G 0 9 C 1/00

H 0 4 L 9/06

9/14

識別記号

庁内整理番号

8837-5L

F I

技術表示箇所

8949-5K

H 0 4 L 9/ 02

Z

審査請求 未請求 請求項の数 1 O L (全 12 頁)

(21)出願番号

特願平5-70436

(22)出願日

平成 5 年(1993) 3 月29日

(71)出願人 000004226

日本電信電話株式会社

東京都千代田区内幸町一丁目 1 番 6 号

(72)発明者 桑門 秀典

東京都千代田区内幸町 1 丁目 1 番 6 号 日  
本電信電話株式会社内

(72)発明者 小山 謙二

東京都千代田区内幸町 1 丁目 1 番 6 号 日  
本電信電話株式会社内

(74)代理人 弁理士 伊東 忠彦

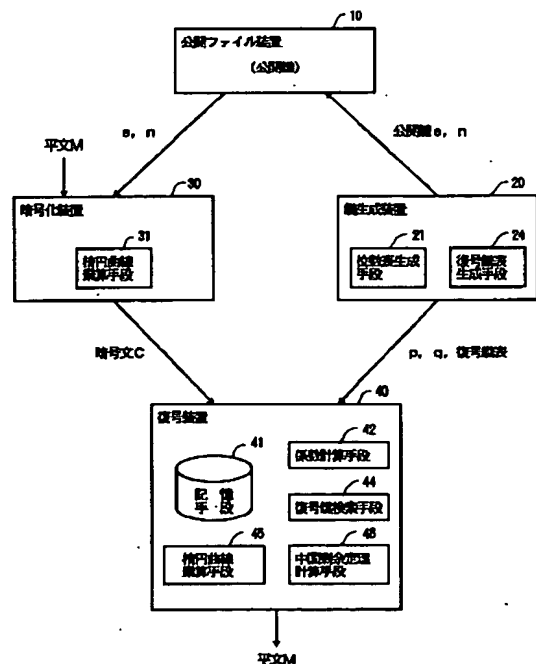
(54)【発明の名称】 楕円曲線に基づく公開鍵暗号方式

(57)【要約】

【目的】 本発明の目的は、パラメータの素数の制限をなくすことにより安全性を一層高めた楕円曲線に基づく公開暗号方式を提供することである。

【構成】 本発明は、任意の素数を選び、素数に対応した暗号化鍵を公開ファイル装置に登録し、素数、暗号鍵に対応する復号鍵表により生成し、素数と共に復号鍵表を復号装置に記憶しておく。暗号化装置は公開ファイル装置より受信者（復号装置）の公開鍵を入手し、平文を楕円曲線上で乗算し、その値を暗号文として復号装置に送信する。復号装置は暗号文から楕円曲線のパラメータを計算し、復号鍵表を用いてパラメータに対応する復号鍵を選び、暗号文をを楕円曲線で乗算した値から中国剰余定理を用いて平文を得る。

本発明の原理構成図



## 【特許請求の範囲】

【請求項1】 受信者により5以上の任意の素数を選択し、該素数に対応する公開鍵を登録する公開ファイル装置と、

素数に対して楕円曲線  $y^2 \equiv x^3 + ax \pmod{n}$  の位数とパラメータとの関係を示す識別子と該位数の対応を示す位数表を生成する位数表生成手段と、該素数と該位数表生成手段により生成された該位数表から復号鍵を計算し、該復号鍵と該位数表の識別子との対応を示す復号鍵表を生成する復号鍵表生成手段とを含む復号表生成装置とを有する鍵生成装置と、

平文と公開鍵が入力され、該平文を楕円曲線  $y^2 \equiv x^3 + ax \pmod{n}$  上で該公開鍵に基づいて乗算する楕円曲線乗算手段を含み、暗号文を出力する暗号化装置と、該素数と復号鍵表を予め記憶しておく記憶手段と、該暗号化装置から取得した該暗号文と該素数から該楕円曲線  $y^2 \equiv x^3 + ax \pmod{n}$  のパラメータを計算する係数計算手段と、該記憶手段に記憶されている該復号鍵表より該楕円曲線  $y^2 \equiv x^3 + ax \pmod{n}$  のパラメータに対応する復号鍵を検索する復号鍵検索手段と、該暗号化装置から入力された該暗号文を該楕円曲線  $y^2 \equiv x^3 + ax \pmod{n}$  上で該復号鍵に基づいて乗算する楕円曲線乗算手段と、該楕円曲線乗算手段により求められた値と該素数から平文を中国剰余定理に基づいて計算し、出力する中国剰余定理計算手段とを含む復号装置とを有することを特徴とする楕円曲線に基づく公開鍵暗号方式。

## 【発明の詳細な説明】

## 【0001】

【産業上の利用分野】 本発明は、楕円曲線に基づく公開鍵暗号方式に係り、特に、デジタル化された文書を伝送する際の暗号方式における有限のモノイド上の楕円曲線に基づく暗号方式及び暗号方式に用いられる鍵生成装置、暗号化装置及び復号装置における楕円曲線に基づく公開鍵暗号方式に関する。

## 【0002】

【従来の技術】 1990年に楕円曲線に基づく公開鍵暗号(KMOV方式)が提案されている。このKMOV方式はパラメータ  $n (=pq)$  の素因数分解の困難さに安全性の根拠をおいているものである。KMOV方式は、パラメータの素数  $p, q$  が  $p \equiv q \equiv 2 \pmod{3}$  または、 $p \equiv q \equiv 3 \pmod{4}$  でなければならないという制限がある。

## 【0003】

【発明が解決しようとする課題】 しかしながら、従来の公開鍵暗号方式にはKMOV方式を用いた方式により暗号方式を用いていたが、法の  $n$  の素因数に制限があるため、この制限内で暗号方式を適用すると鍵の安全性に問題がある。

【0004】 本発明は、上記の点に鑑みなされたもの

で、パラメータの素数の制限をなくすことにより安全性を一層高めた楕円曲線に基づく公開暗号方式を提供することを目的とする。

## 【0005】

【課題を解決するための手段】 図1は本発明の原理構成図を示す。本発明は、受信者により5以上の任意の素数  $p, q$  を選択し、素数  $p, q$  に対応する公開鍵  $e, n$  を登録する公開ファイル装置10と、素数  $p, q$  に対して楕円曲線  $E_p(0, b) : y^2 \equiv x^3 + b_p \pmod{p}$ 、 $E_q(0, b) : y^2 \equiv x^3 + b_q \pmod{q}$  の位数  $b_p, b_q$  とパラメータ  $b$  との関係を示す識別子と位数の対応を示す位数表を生成する位数表生成手段21と、素数  $p, q$  と位数表生成手段21により生成された位数表から復号鍵を計算し、復号鍵と位数表の識別子との対応を示す復号鍵表を生成する復号鍵表生成手段24とを含む鍵生成装置20と、平文  $M$  と受信者の公開鍵  $e, n$  が入力され、平文  $M$  を楕円曲線  $E_n(0, b_M) : y^2 \equiv x^3 + b_M \pmod{n}$  上で公開鍵  $e$  に基づいて乗算する楕円曲線乗算手段31を含み、暗号文を出力する暗号化装置30と、該鍵生成装置20から受け取った素数  $p, q$  と復号鍵表を記憶する記憶手段41と、暗号化装置30からの暗号文  $C$  と素数  $p, q$  から楕円曲線  $E_p(0, b_p) : y^2 \equiv x^3 + b_p \pmod{p}$ 、 $E_q(0, b_q) : y^2 \equiv x^3 + b_q \pmod{q}$  のパラメータ  $b_p, b_q$  を計算する係数計算手段42と、記憶手段41に記憶されている復号鍵表より楕円曲線のパラメータに対応する復号鍵  $d_p, d_q$  を検索する復号鍵検索手段と、暗号化装置30から入力された暗号文  $C$  を楕円曲線  $E_p(0, b_p), E_q(0, b_q)$  上で復号鍵  $d_p, d_q$  に基づいて乗算する楕円曲線乗算手段45と、楕円曲線乗算手段45により求められた値  $M_p, M_q$  と、素数  $p, q$  から平文  $M$  を中国剰余定理に基づいて計算し出力する中国剰余定理計算手段46とを含む復号装置を有する。

## 【0006】

【作用】 本発明は、5以上の任意の素数  $p, q$  を選び、 $p, q$  に対応した暗号化鍵  $e, n$  を公開ファイル装置10に登録し、 $p, q, e$  に対応する復号鍵表を生成し、素数  $p, q$  と共に復号鍵表を復号装置に記憶しておく。送信者(暗号化装置)は公開ファイル装置10より受信者(復号装置)の公開鍵  $e, n$  を入手し、平文  $M = (m_x, m_y)$  を楕円曲線  $E_n(0, b_M) : y^2 \equiv x^3 + b_M \pmod{n}$  上で  $e$  倍した点  $C$  を暗号文  $C$  として受信者(復号装置)に送信する。受信者(復号装置)は暗号文  $C$  から楕円曲線  $E_p(0, b_p) : y^2 \equiv x^3 + b_p \pmod{p}$ 、 $E_q(0, b_q) : y^2 \equiv x^3 + b_q \pmod{q}$  のパラメータ  $b_p, b_q$  を計算し、復号鍵表を用いてパラメータ  $b_p, b_q$  を計算し、復号装置側で予め記憶されている復号鍵表を用いてパラメータ  $b_p, b_q$  に対応する復号鍵  $d_p, d_q$  を選び、暗号文  $C$  を楕円曲

線で $d_p$ ,  $d_q$  倍した点 $M_p$ ,  $M_q$  とから中国剰余定理を用いて明文 $M$ を得る。これにより、公開鍵暗号方式として、従来の $KMOV$ 方式に代わり有限モノイド上の楕円曲線に基づいており、用いる素数に制限がないため、素因数分解が $KMOV$ 方式よりも難解になり、安全性が高くなる。

【0007】

【実施例】以下、図面と共に本発明の実施例を説明する。

【0008】図2は本発明の一実施例のシステム構成を示す。同図のシステムは、公開鍵 $e$ ,  $n$ を登録しておく公開ファイル装置10、公開鍵 $e$ ,  $n$ 及び、復号鍵 $d_p$ ,  $d_q$ を生成する鍵生成装置20、入力された明文 $M$ を公開ファイル装置10からの公開鍵 $e$ ,  $n$ により明文 $M$ を暗号化し、暗号文 $C$ を作成し、出力する暗号化装置30と、暗号化装置30から入力された暗号文 $C$ を楕円曲線を用いて復号し、明文 $M$ を出力する復号装置40から構成される。

【0009】以下、実施例を説明するにあたり、本発明の公開鍵暗号方式における前提条件を説明する。本発明における公開鍵暗号方式は、有限モノイド上の楕円曲線に基づいており、用いる素数に制限のないものである。

【0010】まず、楕円曲線に関する記号の説明をする。素数 $p$ とパラメータ $a$ ,  $b$ に対し、

$$y^2 \equiv x^3 + ax + b \pmod{p}$$

を満たす点の集合に無限遠点 $O$ を加えた集合を楕円曲線 $E_n(a, b)$ と呼ぶ。本発明の実施例ではパラメータ $a$ が零( $a=0$ )の楕円曲線 $E_n(0, b)$ を用いる。

【0011】以下に本発明の一実施例の各装置について説明する。

#### 1. 公開ファイル装置

公開ファイル装置10は、受信者(復号装置)により5以上の任意の素数 $p$ ,  $q$ が選択され、この素数に対応した暗号化鍵(公開鍵) $e$ ,  $n$ が登録される。

#### 【0012】2. 鍵生成装置

図3は本発明の一実施例の鍵生成装置の構成を示す。同図に示す復号鍵生成装置24は、素数生成器241、位数表生成装置242、243及び復号鍵表生成装置244から構成される。素数生成器241は素数 $p$ ,  $q$ を生成し、素数 $p$ を位数表生成装置242に、素数 $q$ を位数表生成装置243に入力する。

#### 【0013】(1) 位数表生成装置

ここで、各位数表生成装置242、243は、素数生成器241から素数 $p$ ,  $q$ により位数表を作成する。位数表生成装置242は、素数 $p$ に対して楕円曲線 $E_p(0, b): y^2 \equiv x^3 + b \pmod{p}$ の位数とパラメータ $b$ との関係を示す識別子と位数の対応を示す位数表を生成する。もし、素数 $p$ が $p \equiv 2 \pmod{3}$

であれば、位数表生成装置242が生成する位数表は、

【0014】

【表1】

識別子	位数
*	$p+1$

【0015】となる。位数表生成装置242は、この位数表を復号鍵表生成装置245に出力する。

【0016】また、位数表生成装置243は素数 $q$ に対して楕円曲線

$$E_q(0, b): y^2 \equiv x^3 + b \pmod{q}$$

の位数とパラメータ $b$ との関係を示す識別子と位数の対応を示す位数表を生成する。もし、素数 $q$ が、

$$q \equiv 2 \pmod{3}$$

であれば、位数表生成装置243が生成する位数表は、

【0017】

【表2】

識別子	位数
*	$q+1$

20 【0018】となり、位数表生成装置243はこの位数表を復号鍵表生成装置245に出力する。

【0019】ここで、位数表生成装置242、243は $p = \pi\pi'$ かつ、 $\pi \equiv 2 \pmod{3}$

を満たす二次体 $Z[\omega]$ 上の整数

$$\pi = \alpha - \beta\omega$$

を求める。この時、位数表生成装置242、243は以下に示す位数表を生成する。

【0020】

【表3】

30

識別子	位数
1	$N_{p0} = p + 1 + (2\alpha + \beta)$
-1	$N_{p1} = p + 1 - (2\alpha + \beta)$
$\omega^2$	$N_{p2} = p + 1 + (\beta - \alpha)$
$-\omega^2$	$N_{p3} = p + 1 - (\beta - \alpha)$
$\omega$	$N_{p4} = p + 1 - (\alpha + 2\beta)$
$-\omega$	$N_{p5} = p + 1 + (\alpha + 2\beta)$

【0021】位数表生成装置242、243は、この位数表を復号鍵表生成装置245に出力し、動作を終了する。

#### 【0022】(2) 復号鍵表生成装置

次に、復号鍵表生成装置245は、2つの素数 $p$ ,  $q$ と各素数の位数表から公開鍵 $e$ ,  $n$ を計算し、復号鍵表を生成し、公開鍵 $e$ ,  $n$ 及び復号鍵表を出力する。

【0023】図4は本発明の一実施例の鍵生成装置の復号鍵表生成装置を説明するための図である。復号鍵表生

50

## 5

成装置 2 4 5 は、素数  $p$ 、 $q$  の入力により使用する復号鍵生成装置 1 ~ 3 を使い分ける。

【0024】 まず、素数  $p$ 、 $q$  が、

$$p \equiv q \equiv 2 \pmod{3}$$

であれば、復号鍵生成装置 1 に素数  $p$ 、 $q$  とそれらの位数表を入力し、復号鍵生成装置 1 の出力をそのまま、復号鍵生成装置 2 4 5 の出力とし、処理を終了する。

【0025】 詳しくは、復号鍵生成装置 1 は、入力として素数  $p$ 、 $q$  と、当該素数  $p$ 、 $q$  の位数表が与えられ

識別子	復号鍵
*	$d_{p0}$

【0027】 とする。但し、これらの表において、左の列の項は識別子を表し、右の列の項はその識別子に対応する復号鍵を表す。これにより復号鍵生成装置 1 は暗号化鍵  $e$ 、 $n$  と復号鍵表を出力する。

【0028】 次に、素数  $p$ 、 $q$  が、

$$p \equiv 1 \pmod{3}, q \equiv 2 \pmod{3}$$

であれば、復号鍵表生成装置 2 に素数  $p$ 、 $q$  とそれらの位数表を入力し、復号鍵表生成装置 2 の出力をそのまま復号鍵表生成装置 2 4 5 の出力とし、処理を終了する。

【0029】 詳しくは、復号鍵生成装置 2 は、入力として素数  $p$ 、 $q$  と、当該素数  $p$ 、 $q$  の位数表が与えられる。ここで、復号鍵生成装置 1 は、

$$\gcd(e, N_{p0}) = \gcd(e, N_{q0})$$

識別子	復号鍵
1	$d_{p0}$
-1	$d_{p1}$
$\omega^2$	$d_{p2}$
$-\omega^2$	$d_{p3}$
$\omega$	$d_{p4}$
$-\omega$	$d_{p5}$

【0032】 とする。但し、これらの表において、左の列の項は識別子を表し、右の列の項はその識別子に対応する復号鍵を表す。これにより復号鍵生成装置 2 は暗号化鍵  $e$ 、 $n$  と復号鍵表を出力する。

【0033】 さらに、素数  $p$ 、 $q$  が

$$p \equiv q \equiv 1 \pmod{3}$$

ならば、復号鍵表生成装置 3 に素数  $p$ 、 $q$  とそれらの位数表を入力し、復号鍵表生成装置 2 4 5 の出力とし、処理を終了する。

## 6

る。ここで、復号鍵生成装置 1 は、

$$\gcd(e, p+1) = \gcd(e, q+1) = 1$$

となる公開鍵  $e$  をランダムに設定する。そして、以下の式を満たす復号鍵  $d_{p0}$ 、 $d_{q0}$  を計算する。

$$e \cdot d_{p0} \equiv 1 \pmod{p}, \quad e \cdot d_{q0} \equiv 1 \pmod{q}$$

これにより、復号鍵生成装置 1 が出力する復号鍵表は、

【0026】

【表 4】

識別子	復号鍵
*	$d_{q0}$

$$= \gcd(e, N_{p1})$$

$$= \gcd(e, N_{p2})$$

$$= \gcd(e, N_{p3})$$

$$= (e, q+1)$$

$$= 1$$

20 となる公開鍵  $e$  をランダムに設定する。そして、以下の式を満たす復号鍵  $d_{pi}$  ( $i=0 \sim 3$ )、 $d_{q0}$  を計算する。

$$【0030】 e \cdot d_{pi} \equiv 1 \pmod{p} \quad (i=0 \sim 3),$$

$$e \cdot d_{q0} \equiv 1 \pmod{q}.$$

これにより、復号鍵生成装置 2 が出力する復号鍵表は、

【0031】

【表 5】

識別子	復号鍵
*	$d_{q0}$

【0034】 詳しくは、復号鍵生成装置 3 は、入力として素数  $p$ 、 $q$  と、当該素数  $p$ 、 $q$  の位数表が与えられる。ここで、復号鍵生成装置 1 は、

$$\gcd(e, N_{pi}) = \gcd(e, N_{pi})$$

$$= 1 \quad (i=0 \sim 3)$$

となる公開鍵  $e$  をランダムに設定する。そして、以下の式を満たす復号鍵  $d_{pi}$ 、 $d_{qi}$  を計算する。

$$【0035】 e \cdot d_{pi} \equiv 1 \pmod{p}$$

$$50 \quad e \cdot d_{qi} \equiv 1 \pmod{q} \quad (i=0 \sim 3).$$

これにより、復号鍵生成装置 3 が出力する復号鍵表は、  
【0036】

識別子	復号鍵
1	$d_{p0}$
-1	$d_{p1}$
$\omega^2$	$d_{p2}$
$-\omega^2$	$d_{p3}$
$\omega$	$d_{p4}$
$-\omega$	$d_{p5}$

【0037】とする。但し、これらの表において、左の列の項は識別子を表し、右の列の項はその識別子に対応する復号鍵を表す。

【0038】これにより復号鍵生成装置 3 は暗号化鍵  $e$ 、 $n$  と復号鍵表を公開ファイル装置 10 または、復号装置 40 に出力する。

【0039】(3) 暗号化装置

図 5 は本発明の一実施例の暗号化装置の構成を示す。暗号化装置 30 は楕円曲線  $E_n(0, b_M)$  上において入力された明文  $M$  に公開鍵  $e$  分を乗算する楕円曲線乗算器 31 を有する。

【0040】暗号化装置 30 は、入力として、公開鍵  $e$ 、 $n$  と明文  $M = (m_x, m_y)$  が与えられる。但し、 $0 < m_x, m_y < n$  and  $\gcd(m_x, n) = \gcd(m_y, n) = 1$  とする。

【0041】暗号化装置 30 は、楕円曲線  $E_n(0, b_M) : y^2 \equiv x^3 + b_M \pmod{n}$  上で、 $e \cdot m$  over  $E_n(0, b_M)$

を計算し、その計算結果を暗号文  $C$  とする。そして、暗号文  $C$  を復号装置 40 に出力して処理を終了する。

【0042】(4) 復号装置

図 6 は本発明の一実施例の復号装置の構成を示す。同図において、復号装置 40 は、素数  $p$  記憶部 410、素数  $q$  記憶部 411、第 1、第 2 の係数計算器 420、421、第 1、第 2 の識別子計算器 430、431、復号鍵検索器 440、441、第 1、第 2 の楕円曲線乗算器 450、451、 $p$  の復号鍵表記憶部 470、 $q$  の復号鍵記憶部 471 及び中国剰余定理計算器 460 より構成される。

【0043】復号装置 40 の素数  $p$  記憶部 410 は素数  $p$  を記憶しておき、素数  $q$  記憶部 411 は素数  $q$  を記憶しておく。

【0044】第 1 の係数計算器 420 は、暗号化装置 30 から入力された暗号文  $C$  と素数  $p$  記憶部 410 に記憶

【表 6】

識別子	復号鍵
1	$d_{q0}$
-1	$d_{q1}$
$\omega^2$	$d_{q2}$
$-\omega^2$	$d_{q3}$
$\omega$	$d_{q4}$
$-\omega$	$d_{q5}$

されている素数  $p$  から楕円曲線

$$E_p(0, b_p) : y^2 \equiv x^3 + b_p \pmod{p}$$

のパラメータ  $b_p$  を計算する。

【0045】第 2 の係数計算器 421 は、暗号化装置 30 から入力された暗号文  $C$  と素数  $q$  記憶部 411 に記憶されている素数  $q$  から楕円曲線

$$E_q(0, b_q) : y^2 \equiv x^3 + b_q \pmod{q}$$

のパラメータ  $b_q$  を計算する。

【0046】第 1 の識別子計算器 430 は、楕円曲線のパラメータ  $b_p$  と素数  $p$  から識別子  $\tau_p$  を計算する。

【0047】第 2 の識別子計算器 431 は、楕円曲線のパラメータ  $b_q$  と素数  $q$  から識別子  $\tau_q$  を計算する。

【0048】 $p$  の復号鍵表記憶部 470 は、素数  $p$  の復号鍵表を記憶し、 $q$  の復号鍵表記憶部 471 は素数  $q$  の復号鍵表を記憶する。

【0049】復号鍵検索器 440 は  $p$  の復号鍵表記憶部 470 からの復号鍵表と第 1 の識別子計算器 430 から識別子  $\tau_p$  が入力されると、当該識別子  $\tau_p$  により復号鍵表を検索し、復号鍵  $d_p$  を取得する。

【0050】復号鍵検索器 441 は識別子  $q$  が入力されると、当該識別子  $\tau_q$  により復号鍵表を検索し、復号鍵  $d_q$  を取得する。

【0051】第 1 の楕円曲線乗算部 450 は、暗号化装置 30 から入力された暗号文  $C$  を楕円曲線  $E_p(0, b_p)$  上で  $d_p$  倍して、乗算された結果  $M_p$  を出力する。

【0052】第 2 の楕円曲線乗算部 451 は、暗号化装置 30 から入力された暗号文  $C$  を楕円曲線  $E_q(0, b_q)$  上で  $d_q$  倍して、乗算された結果  $M_q$  を出力する。

【0053】中国剰余定理計算器 460 は素数  $p$  記憶部 410 からの素数  $p$  と素数  $q$  記憶部 411 からの素数  $q$  と第 1 の楕円曲線乗算器 450、第 2 の楕円曲線乗算器 451 から  $M_p$ 、 $M_q$  が入力されると、中国剰余定理により、明文  $M$  を出力する。

【0054】詳しくは、復号装置 40 は、入力として、暗号化装置 30 から暗号文  $C = (c_x, c_y)$  が与えら

れ、第1及び第2の係数計算器420、421では、パラメータ

$$b_p = c_y^2 - c_x^3 \pmod{p},$$

$$b_q = c_y^2 - c_x^3 \pmod{q}$$

を計算する。

【0055】第1及び第2の識別子計算器430、431は、各パラメータ $b_p$ 、 $b_q$ と、各素数記憶部410、411から得られた素数によりもし、 $p \equiv q \equiv 2 \pmod{3}$ であれば、素数 $p$ に対する識別子を「\*」、素数 $q$ に対する識別子を「\*」とする。また、 $p \equiv 1 \pmod{3}$ 、 $q \equiv 2 \pmod{3}$ ならば、素数 $p$ に対する識別子 $\tau_p$ を、

【0056】

【数1】

$$\tau_p = \left( \frac{4b_p}{\pi p} \right) 6$$

の計算結果とし、素数 $q$ に対する識別子 $\tau_q$ を、

【0057】

【数2】

$$\tau_q = \left( \frac{4b_q}{\pi q} \right) 6$$

【0058】とし、各々の計算結果を素数 $p$ に対する識別子 $\tau_p$ 、素数 $q$ に対する識別子 $\tau_q$ とする。復号鍵検索器440、441は、 $p$ 、 $q$ の復号鍵表記録部470、471から復号鍵表を識別子 $\tau_p$ 、 $\tau_q$ により検索し、復号鍵 $d_p$ 、 $d_q$ を得る。次に、第1の楕円曲線乗算器450、451は、楕円曲線

$$E_p(0, b_p) : y^2 \equiv x^3 + b_p \pmod{p}$$

$$E_q(0, b_q) : y^2 \equiv x^3 + b_q \pmod{q}$$

上において、

$$d_p \cdot C \text{ over } E_p(0, b_p),$$

$$d_q \cdot C \text{ over } E_q(0, b_q)$$

を計算し、各々の計算結果を $M_p$ 、 $M_q$ とする。これにより、中国剰余定理計算器460は中国剰余定理を用いて $M_p$ 、 $M_q$ より平文 $M$ を計算し、平文 $M$ として出力する。

【0059】なお、上記実施例の中の説明で用いられている素数 $p$ 、 $q$ の桁数は、その積 $n (= pq)$ の素因数分解の困難さを考慮して決められる。

【0060】

【発明の効果】上述のように本発明によれば、法 $n$ の素因数 $p$ 、 $q$ に制限がないため、その素因数分解がより難しく、素数 $p$ 、 $q$ の大きさを同じにした場合に、KM OV方式に比べてより安全である。これにより、安全な公開鍵暗号方式を提供することができる。

【図面の簡単な説明】

【図1】本発明の原理構成図である。

【図2】本発明の一実施例のシステム構成図である。

【図3】本発明の一実施例の鍵生成装置の構成図である。

【図4】本発明の一実施例の復号鍵表生成装置を説明するための図である。

【図5】本発明の一実施例の暗号化装置の構成図である。

【図6】本発明の一実施例の復号装置の構成図である。

【符号の説明】

1, 2, 3 復号鍵生成装置

10 公開ファイル装置

20 鍵生成装置

21 位数表生成手段

24 復号鍵生成手段

30 暗号化装置

31, 45 楕円曲線乗算手段

40 復号装置

41 記憶手段

42 係数計算手段

43 識別子計算手段

44 復号鍵検索手段

30 46 中国剰余定理計算手段

241 素数生成器

242, 243 位数表生成装置

245 復号鍵表生成装置

410 素数 $p$ 記憶部

411 素数 $q$ 記憶部

420 第1の係数計算器

421 第2の係数計算器

430 第1の識別子計算器

431 第2の識別子計算器

40 440, 441 復号鍵検索器

450 第1の楕円曲線乗算器

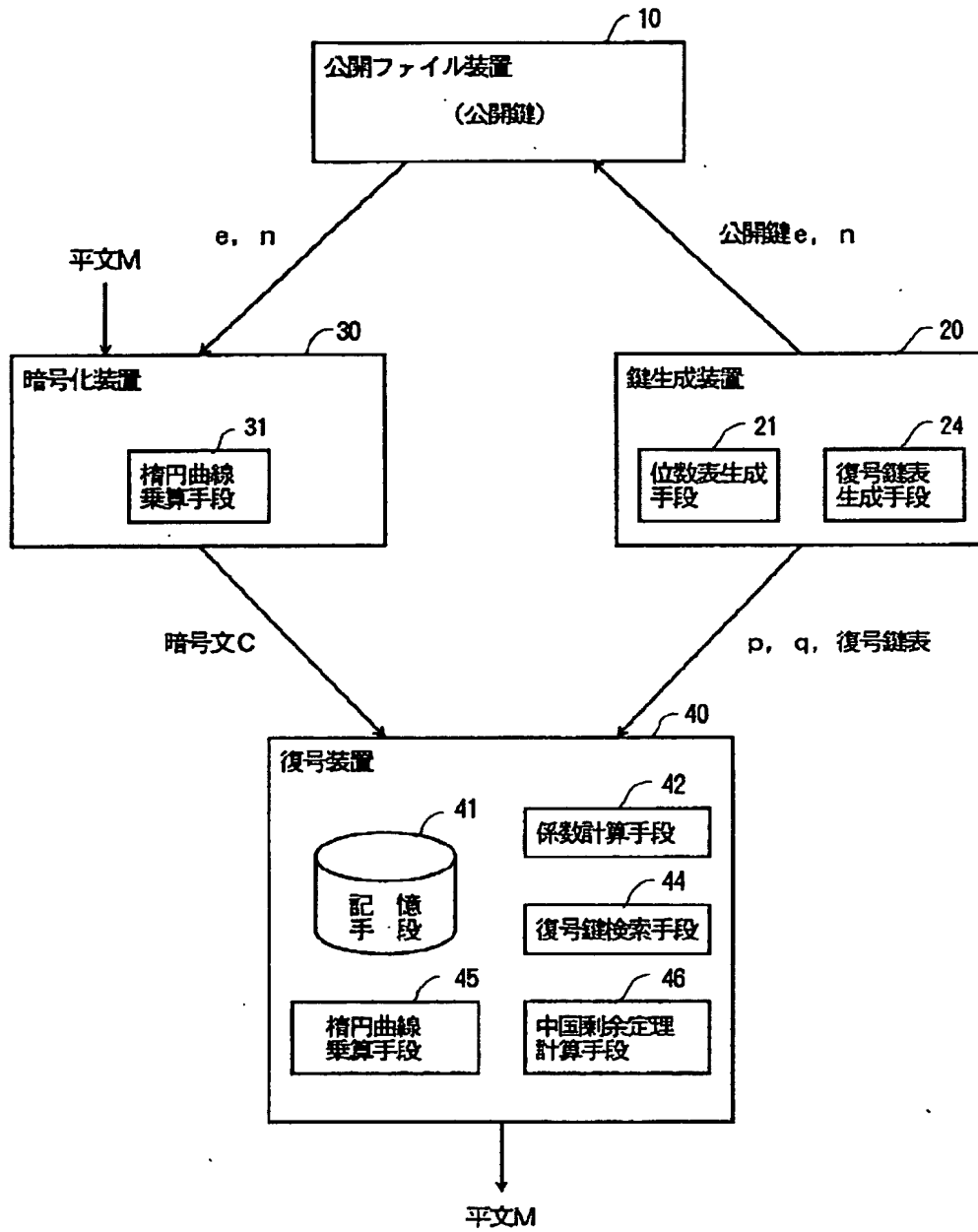
451 第2の楕円曲線乗算器

460 中国剰余定理計算器



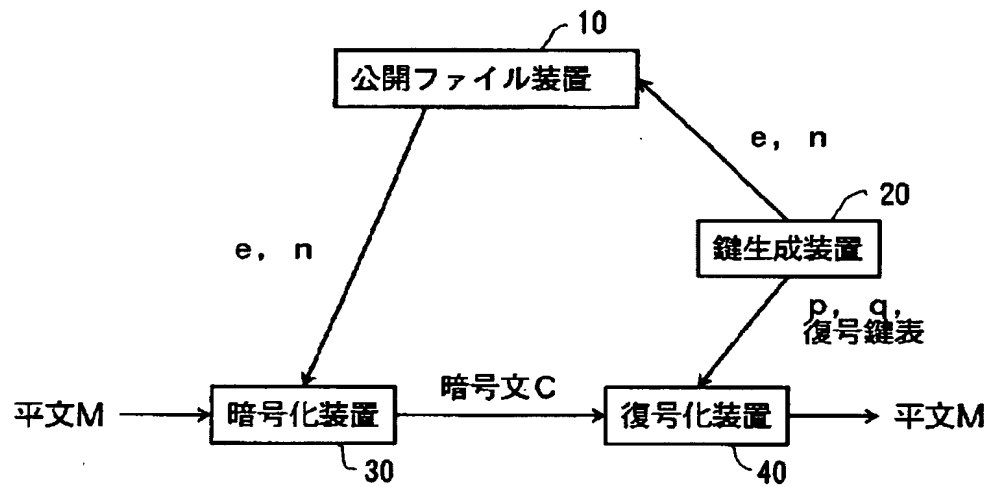
【図1】

## 本発明の原理構成図



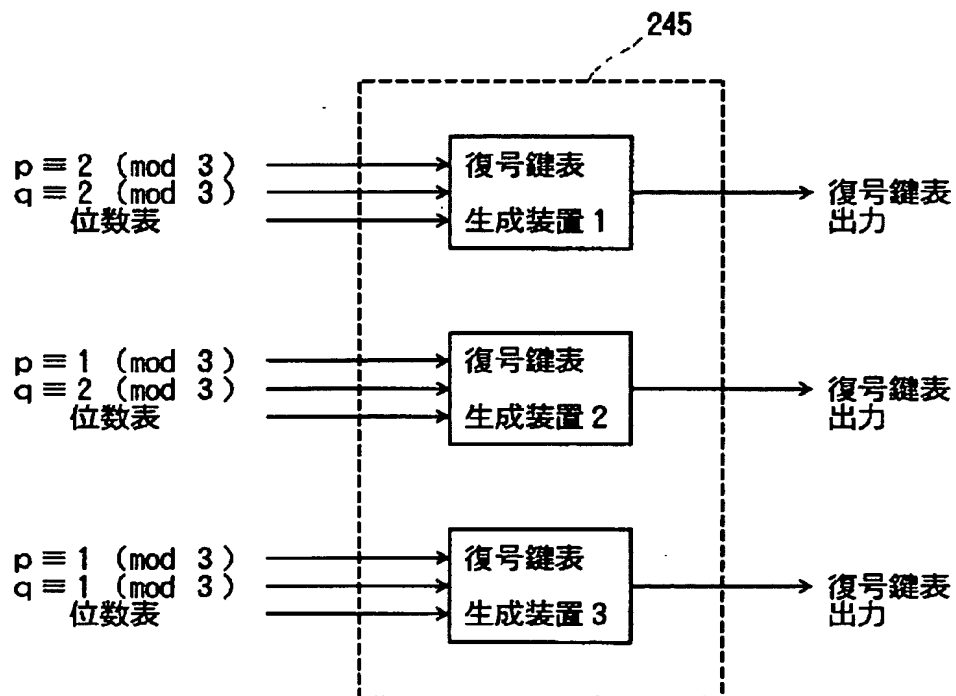
【図2】

本発明の一実施例のシステム構成図



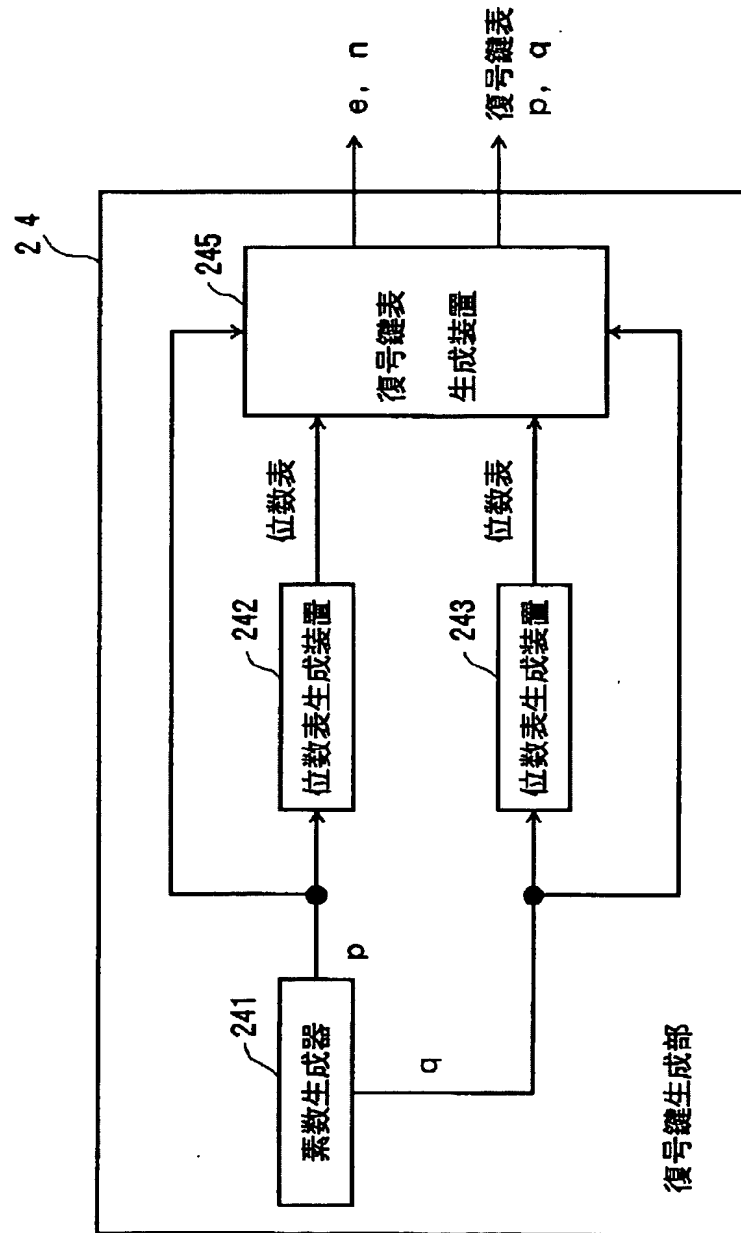
【図4】

本発明の一実施例の復号鍵表生成装置を  
説明するための図



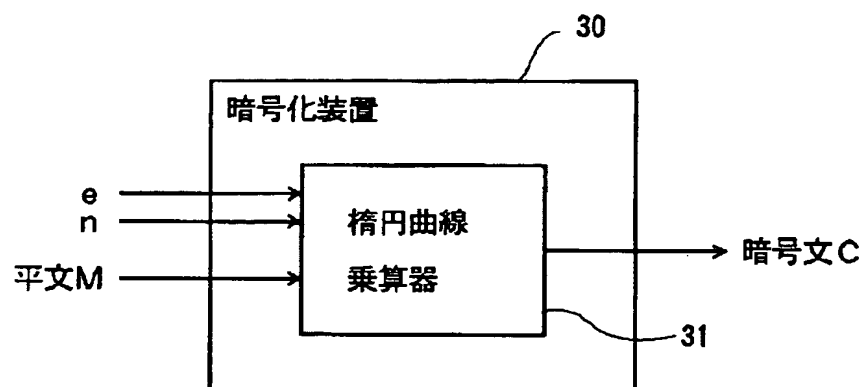
【図3】

## 本発明の一実施例の鍵生成装置の構成図



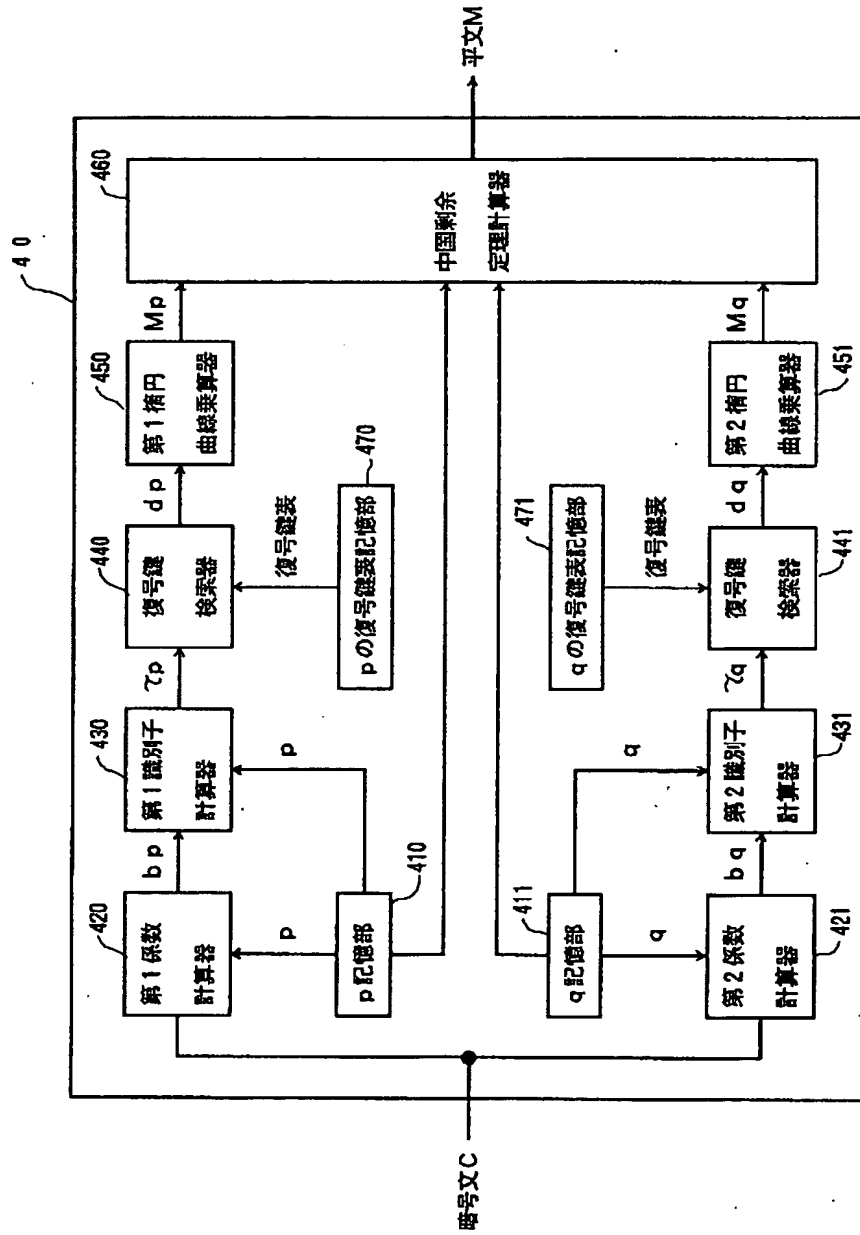
【図5】

## 本発明の一実施例の暗号化装置の構成図



【図6】

## 本発明の一実施例の復号装置の構成図



【手続補正書】

【提出日】平成 5 年 5 月 7 日

【手続補正 1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正内容】

【特許請求の範囲】

【請求項 1】 受信者により 5 以上の任意の素数を選択し、該素数に対応する公開鍵を登録する公開ファイル装置と、

素数に対して楕円曲線  $y^2 \equiv x^3 + b \pmod{n}$  の位数とパラメータとの関係を示す識別子と該位数の対応を示す位数表を生成する位数表生成手段と、該素数と該位数表生成手段により生成された該位数表から復号鍵を計算し、該復号鍵と該位数表の識別子との対応を示す復号鍵表を生成する復号鍵表生成手段とを含む復号表生成装置

とを有する鍵生成装置と、

平文と公開鍵が入力され、該平文を楕円曲線  $y^2 \equiv x^3 + b \pmod{n}$  上で該公開鍵に基づいて乗算する楕円曲線乗算手段を含み、暗号文を出力する暗号化装置と、該素数と復号鍵表を予め記憶しておく記憶手段と、該暗号化装置から取得した該暗号文と該素数から該楕円曲線  $y^2 \equiv x^3 + b \pmod{n}$  のパラメータを計算する係数計算手段と、該記憶手段に記憶されている該復号鍵表より該楕円曲線  $y^2 \equiv x^3 + b \pmod{n}$  のパラメータに対応する復号鍵を検索する復号鍵検索手段と、該暗号化装置から入力された該暗号文を該楕円曲線  $y^2 \equiv x^3 + b \pmod{n}$  上で該復号鍵に基づいて乗算する楕円曲線乗算手段と、該楕円曲線乗算手段により求められた値と該素数から平文を中国剰余定理に基づいて計算し、出力する中国剰余定理計算手段とを含む復号装置とを有することを特徴とする楕円曲線に基づく公開鍵暗号方式。